UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/558,942	08/21/2006	Gary Paul Noble	GB920030011US1	7231

45832 7590 07/23/2010

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/23/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/558,942	NOBLE, GARY PAUL	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 May 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-12,16-20 and 22-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 8-12, 16-20, 22-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 21 May 2010, has been entered into record. In this amendment, claims 1-5, 8-12, 16-20, and 22-24 have been amended, and claims 6, 7, 13-15, and 21 have been canceled.

2. Claims 1-5, 8-12, 16-20, and 22-24 are presented for examination.

Response to Arguments

3. With regards to the objections to the specification, claims, and drawings, the applicant has filed amendments, and the examiner hereby withdraws the objections.

4. Applicant's arguments filed 21 May 2010 have been fully considered but they are not persuasive.

In response to applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, the teachings of both Batten-Carew and Kudo relate to protecting data using encryption and decryption with keys. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide further protection for the

recipient of the data by protecting the key, as disclosed by Kudo (0003, lines 4-10; 0004, lines 4-5).

As to claims 1, 9, 20, 23, and 24, it is argued by the applicant that Kudo does not disclose multiple publishers that each have a password issued by a trusted body for preventing disclosure of a decryption key. The examiner respectfully disagrees. Kudo discloses that the decryption key is only transmitted to a particular user under certain conditions (0020, lines 10-12) and that the encrypted message is only transmitted if a digital signature of that particular user is verified (0003, lines 4-10).

The applicant argues that the name of Kudo does not correspond to the password of the claimed invention. The examiner respectfully disagrees. It is noted that the claims do not provide further description of the password; therefore, the examiner has interpreted the name of Kudo as the password of the claimed invention.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5, 9-12, 19, 20, 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew et al. (US Patent 6,603,857 B1) and Batten-Carew hereinafter) in view of Kudo et al. (US 2001/0052071 A1 and Kudo hereinafter). As to claims 1, 23, and 24, Batten-Carew discloses:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (col. 3, lines 39-47)**;**

the publisher using the encryption key to encrypt data (col. 3, lines 50-51)**;**

the recipient obtaining the encrypted data (col. 3, lines 51-54)**;**

the trusted body making the decryption key available to the recipient at the specified date and time (col. 3, lines 57-61)**, wherein the trusted body generates one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers** (col. 3, lines 44-47)**.**

Batten-Carew fails to specifically disclose:

the trusted body providing a digital certificate signed with a private key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption k prior to the specified date and time;

each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses a system and method for time-dependent decryption, the system and method having:

the trusted body providing a digital certificate signed with a key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption k prior to the specified date and time (0003, lines 4-10; 0061, lines 10-13; 0065, lines 1-5), but does not explicitly disclose where the digital certificate is signed with a private key.

each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key (0003, lines 4-10).

It is well known in the art that signed documents in a public-key cryptography system are signed using a private key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is signed with a key, it is signed with a private key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by providing an encryption key through a digital certificate prior to a specified time and issuing a password. Kudo recites motivation by disclosing that providing keys in a time-key certificate guarantees that a time for enabling decryption information is limited (0019, lines 1-6). Kudo also discloses that each certificate contains the name of the user used to confirm that the certification authority has provided the digital signature for the public encryption key for that user, guaranteeing that no person other than that user can decrypt the encrypted

data (0003, lines 4-10; 0004, lines 4-5). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by providing an encryption key in a certificate and issuing a password in order to limit the time for enabling decryption information and guarantee that no other user can decrypt the data.

As to claim 9, Batten-Carew discloses:

a publisher (i.e. end user) (col. 3, lines 50-52)**;**

a trusted body (i.e. server) (col. 3, lines 35-37)**;**

an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (col. 3, lines 39-47)**;**

means for making the decryption key available at the specified date and time (col. 3, lines 57-61)**, wherein there is a plurality of publishers, one or more asymmetrical key pairs for the specified date and time, a different asymmetrical key pair for each of the plurality of publishers** (col. 2, lines 35-37; col. 3, lines 25-28, 35-47)**.**

Batten-Carew fails to specifically disclose:

a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time;

each of the plurality of publishers has a password issued by the trusted body for preventing the disclosure of the decryption key.

Nonetheless, these features are known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

> **a digital certificate signed with a key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time** (0003, lines 4-10; 0061, lines 10-13; 0065, lines 1-5), but does not explicitly disclose where the digital certificate is signed with a private key.
>
> **each of the plurality of publishers has a password issued by the trusted body for preventing the disclosure of the decryption key** (0003, lines 4-10).

It is well known in the art that signed documents in a public-key cryptography system are signed using a private key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is signed with a key, it is signed with a private key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by providing an encryption key using a digital certificate prior to a specified time and issuing a password. Please refer to the motivation recited above with respect to claims 1 and 24 are to why it is obvious to apply the teachings of Kudo to the teachings of Batten-Carew.

As to claim 2, Batten-Carew fails to specifically disclose:

> **wherein the publisher verifies the signature on the digital certificate with the public key of the trusted body.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

> **wherein the publisher verifies the signature on the digital certificate with the key of the trusted body** (0065, lines 1-5)**,** but does not explicitly disclose where the digital certificate is verified with a public key.

It is well known in the art that signed documents in a public-key cryptography system are verified using a public key, as evidenced by Schneier (page 37, lines 26-30; page 185, lines 38-39; page 186, lines 1-7). Therefore, since Kudo discloses that the digital certificate is verified with a key, it is verified with a public key.

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by verifying the signature on the certificate. Kudo recites motivation by disclosing that verifying the correct signature allows for the user to trust the decryption condition service provided by the time-key certificate manager (0024, lines 1-5). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by verifying the signature of a digital certificate in order to establish trust with the decryption condition service of the time-key certificate manager.

As to claims 3 and 12, Batten-Carew discloses:

wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure (col. 3, lines 44-47).

As to claim 4, Batten-Carew discloses:

wherein the trusted body creates the asymmetrical key pair for the specified date and time on demand from a publisher (col. 3, lines 35-40).

As to claim 5, Batten-Carew discloses:

wherein the trusted body generates one key pair for the specified date and time (col. 3, lines 35-40).

As to claim 10, Batten-Carew discloses:

including one or more recipients with means for obtaining data encrypted with the encryption key from the publisher prior to the specified date and time and means for obtaining the decryption key at or after the specified date and time (col. 3, lines 51-54, 57-61).

As to claim 11, Batten-Carew fails to specifically disclose:

wherein the certificate includes the specified date and time, the encryption key, and a name of the trusted body.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

> **wherein the certificate includes the specified date and time, the encryption key, and a name of the trusted body** (0003, lines 4-10; 0005, lines 4-7)**.**

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by including a specified time, encryption key, and trusted body name in the certificate. Kudo recites motivation by disclosing that using a certificate guarantees that no other person can decrypt the data while limiting the time for enabling the decryption (0004, lines 4-5; 0019, lines 1-6). It is obvious that the teachings of Kudo would have improved the teachings of Batten-Carew by including a specified time, encryption key, and trusted body name in the certificate in order to limit who may decrypt the information and when the information may be decrypted.

As to claim 19, Batten-Carew discloses:

> **wherein the trusted body** (i.e. server) **is accessible by the publisher** (i.e. end users) **and the recipients via a communication network** (col. 2, lines 35-37; col. 3, lines 50-54)**.**

As to claim 20, Batten-Carew discloses:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (col. 3, lines 39-47);

the trusted body providing the publisher with the encryption key prior to the specified date and time (col. 3, lines 48-49);

the publisher using the encryption key to encrypt data (col. 3, lines 50-51);

the recipient obtaining the encrypted data (col. 3, lines 51-54);

the trusted body making the decryption key available to the recipient at the specified date and time (col. 3, lines 57-61);

wherein the trusted body generates one or more asymmetrical key pairs for a specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers (col. 2, lines 35-37; col. 3, lines 25-28, 35-47).

Batten-Carew fails to specifically disclose:

wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew, as taught by Kudo.

Kudo discloses:

wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key (0003, lines 4-10)**.**

Given the teaching of Kudo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew with the teachings of Kudo by preventing disclosure of the decryption key using a password. Please refer to the motivation recited above with respect to claims 1 and 24 are to why it is obvious to apply the teachings of Kudo to the teachings of Batten-Carew.

7. Claims 8, 16-18, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Batten-Carew in view of Kudo as applied to claims 1, 9, and 20 above, and further in view of Di Crescenzo et al. (US Patent 6,813,358 B1 and Di Crescenzo hereinafter).

As to claims 8, 16, and 22, Batten-Carew in view of Kudo fails to specifically disclose:

wherein the decryption key is encrypted with a public key and only the recipient with a corresponding private key can obtain the decryption key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses a system and method for timed-release cryptosystems, the system and method having:

> **wherein the decryption key is encrypted with a public key and only the recipient with a corresponding private key can obtain the decryption key** (col. 2, lines 44-45)**.**

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di Crescenzo by encrypting the decryption key with a public key. Di Crescenzo recites motivation by disclosing that encrypting the decryption key allows a receiver to decrypt the data only after a release time without establishing communication between the sender and the server (col. 2, lines 17-23). It is obvious that the teachings of Di Crescenzo would have improved the teachings of Batten-Carew in view of Kudo by encrypting a decryption key with a public key in order to provide the decryption key after a release time without establishing communication between the sender and server.

As to claim 17, Batten-Carew in view of Kudo fails to specifically disclose:

> **wherein the trusted body has one or more agents who act on behalf of the trusted body.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses:

wherein the trusted body has one or more agents who act on behalf of the trusted body (col. 2, lines 48-51; col. 4, lines 47-55).

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di Crescenzo by using a smart card agent for the trusted body. Di Crescenzo recites motivation by disclosing that senders, receivers, and time servers may include any computer and/or processing device such as desktop computers, portable computers, and/or smart cards in order to provide for timed-release data (col. 4, lines 40-55). It is obvious that the teachings of Di Crescenzo would have improved the teachings of Batten-Carew in view of Kudo by using a smart card as an agent in order to provide for the timed-release of data.

As to claim 18, Batten-Carew in view of Kudo fails to specifically disclose:

wherein an agent for the trusted body is a smart card having an internal clock for providing the decryption key to a recipient.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Batten-Carew in view of Kudo, as taught by Di Crescenzo.

Di Crescenzo discloses:

wherein an agent for the trusted body (i.e. server) **is a smart card having an internal clock for providing the decryption key to a recipient** (i.e. receiver) (col. 2, lines 48-51; col. 4, lines 47-55)**.**

Given the teaching of Di Crescenzo, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Batten-Carew in view of Kudo with the teachings of Di Crescenzo by using a smart card agent for the trusted body. Please refer to the motivation recited above with respect to claim 17 as to why it is obvious to apply the teachings of Di Crescenzo to the teachings of Batten-Carew in view of Kudo.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431